UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

VALERIE GRIFFITH-SULLIVAN, Individually and on Behalf of All Similarly Situated Persons, Plaintiff, v. LUMICO LIFE INSURANCE COMPANY, Defendant.	**Civil Action No.:** 23-cv-10880 PROPOSED CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Valerie Griffith-Sullivan ("Plaintiff") brings this Class Action Complaint against Lumico Life Insurance Company ("Lumico" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personal identifiable information ("PII")[1] of more than 1,300 individuals, including, but not limited to, name, gender, Social Security number, date of birth, address, and policy numbers.

2. Defendant sells life insurance, including term life policies and whole life policies.

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. §200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

3. Defendant's Privacy Policy states as follows:

> We are committed to keeping the non-public personal information ("NPI") we collect confidential and secure. . . . Our Privacy Policy applies to potential, current and former customers . . . . We disclose your NPI only as permitted or required by law . . . . We maintain physical, electronic, and procedural safeguards to protect your NPI . . . . Some examples of what we may collect: Data you provide on applications (name, address, date of birth, Social Security number, income, and beneficiary) . . . .

4. Prior to and through May 30, 2023, Defendant obtained the PII of Plaintiff and Class Members, including by collecting it directly from Plaintiff and Class Members. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. Prior to and through May 30, 2023, Defendant shared the PII of Plaintiff and Class Members, unencrypted, with its third-party service provider, NTT Data Services ("NTT").

6. Prior to and through May 30, 2023, NTT shared the PII of Plaintiff and Class Members, unencrypted, with Pension Benefits Information, LLC ("PBI"), ostensibly to perform regulatory compliance and operational-support services.

7. On or before June 19, 2023, Defendant learned of a data breach involving the "MOVEit" secure file-transfer application, which PBI used (the "Data Breach").

8. Defendant determined that, during the Data Breach, an unknown actor may have acquired the unencrypted PII of Plaintiff and Class Members.

9. On or around July 24, 2023, Defendant began notifying various states' Attorneys General of the Data Breach.

10. On or around July 24, 2023, Defendant began notifying Plaintiff and Class Members of the Data Breach.

11. Defendant admits that the unencrypted PII that was accessed and/or acquired by an unauthorized actor included name, gender, Social Security number, date of birth, address, and policy numbers.

12. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members now face a lifetime risk of: (i) identity theft, which is heightened here by the loss of Social Security numbers; and (ii) the sharing and detrimental use of their sensitive information.

13. The PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members, including the failure to encrypt the PII and the failure to ensure that entities with which Defendant shared the PII maintained it in encrypted form.

14. As a result of the Data Breach, Plaintiff and Class Members are, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

15. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; and (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices. Defendant's conduct amounts to negligence and violates federal and state statutes.

16. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use

of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

17. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

18. Plaintiff Valerie Griffith-Sullivan is a citizen of California residing in Roseville, California. Griffith-Sullivan received Notice of the Data Breach from Lumico on July 24, 2023. The Notice informed her that her name, gender, Social Security number, date of birth, address, and policy numbers, and possible other information, was taken in the breach. Since the Data Breach, Griffith-Sullivan received reports that her personal information is on the dark web. Griffith-Sullivan spent significant time responding to the Data Breach, including contacting all major credit bureaus and filing a police report. This time has been lost forever and cannot be recaptured. Griffith-Sullivan

is very careful about sharing her own PII. She diligently chooses unique usernames and passwords for her various online accounts. She estimates she spends an extra hour or two per week remaining extra vigilant regarding her credit, reviewing her accounts, and researching the effects of the Data Breach.

19. Defendant is a Missouri corporation with a principal place of business in Armonk, New York.

20. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

21. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

22. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. §1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs; there are more than 100 members in the proposed class; and at least one Class Member, including Plaintiff, is a citizen of a state different from Defendant to establish minimal diversity.

23. Defendant is a citizen of Missouri and New York because it is a corporation formed under Missouri law with its principal place of business in Armonk, New York.

24. The Southern District of New York has personal jurisdiction over Defendant because it conducts substantial business in New York and this District, and it collected and/or stored the PII of Plaintiff and Class Members in this District.

25. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, including Defendant collecting and/or storing the PII of Plaintiff and Class Members.

FACTUAL ALLEGATIONS

Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII

26. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members and shared it, unencrypted, with NTT, which in turn shared it with PBI.

27. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from involuntary disclosure to third parties.

28. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

The Data Breach

29. On or about July 24, 2023, Defendant sent Plaintiff and Class Members a *Notice of Security Incident* and submitted sample notices to various states' Attorneys General. Defendant informed Plaintiff and other Class Members that:

> The Lumico Life Insurance Company is writing to let you know about a third-party software vulnerability that impacted some of your information. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect yourself.

What Happened? Progress Software disclosed that cyber criminals actively exploited a vulnerability in the MOVEit Transfer application. Because thousands of organizations use MOVEit to support secure file transfers, this incident has affected many companies around the world, including our third-party service provider NTT Data Services ("NTT"), and has been the subject of widespread media coverage.

On June 19, 2023, NTT informed us that, between May 29 and 30 of this year, an unauthorized third party exploited the vulnerability in the MOVEit application, which NTT's external vendor Pension Benefits Information, LLC ("PBI") uses, and may have acquired some of our policyholder information. For context, we provide NTT with policyholder data that it shares with PBI to perform regulatory compliance and operational support services for the benefit of our policies.

As explained to us by NTT, PBI completed the recommended patching and remediation steps to secure its systems on June 2 and has informed law enforcement of the incident. On June 30, our review of the data provided by NTT determined that the unauthorized third party in fact had acquired some of our policyholder information, as listed below.

The incident occurred entirely within PBI's systems, and we have no reason to believe that it impacted our own systems or network environment. As noted, we are also one of many companies affected by the incident, and we have no reason to believe that our policyholder data was specifically targeted.

What Information Was Involved? Based on our analysis, we believe the following types of information related to you were impacted:

- Contact information, including name;
- Gender;
- Social Security number;
- Date of birth;
- Address; and
- Policy numbers.[2]

30. Plaintiff's *Notice of Security Incident* states that her name, gender, Social Security number, date of birth, address, and policy numbers were impacted in the Data Breach.

[2] Exhibit 1 at 2 (sample Notice of Data Security Incident filed with California Attorney General), filed concurrently herewith.

31. Defendant admitted in the *Notice of Security Incident* and the sample notices and reports it sent to the states' Attorneys General that an unauthorized actor may have acquired sensitive information about Plaintiff and Class Members, including name, gender, Social Security number, date of birth, address, and policy numbers.

32. In response to the Data Breach, Defendant claims that it "activated [its] incident response protocols and took prompt steps to ensure the ongoing security of [its] policyholder information."[3]

33. However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

34. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack on third parties with which Defendant shared the PII.

35. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack on third parties with which Defendant shared the PII.

36. Prior to the Data Breach, Defendant knew or should have known that it should have ensured that third parties with which it shared the PII encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

---

[3] *Id.*

37. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of PII for Plaintiff and Class Members.

38. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

Securing PII and Preventing Breaches

39. Defendant could have prevented this Data Breach by properly encrypting the PII of Plaintiff and Class Members and ensuring that third parties with which Defendant shared the PII maintained it in encrypted form.

40. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

41. Despite the prevalence of public announcements of data breaches and data-security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

42. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[4] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's

[4] 17 C.F.R. §248.201 (2013).

license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[5]

43. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

44. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark-web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[6] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[7] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[8]

45. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit-card information in a retailer data breach because, there, victims can cancel or close credit- and debit-card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

---

5 *Id*.

6 Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

7 Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

8 *In the Dark*, VPNOVERVIEW, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Dec. 14, 2023).

46. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "'Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x in price on the black market.'"[9]

47. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing, or even give false information to police.

48. The fraudulent activity resulting from the Data Breach may not come to light for years.

49. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[10]

50. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

51. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security

---

[9] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, NETWORK WORLD (Feb. 6, 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[10] *Report to Congressional Requesters (No. GAO-07-737)*, UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

numbers, and of the foreseeable consequences that would occur from the breach of a data security system of a third party with which Defendant shared the PII, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

52. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in the PII it shared with NTT and PBI, amounting to thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

53. To date, Defendant has offered Plaintiff and Class Members two years of identity monitoring through Kroll. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

54. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff's Experience

55. Plaintiff obtained life insurance from Defendant prior to the Data Breach and received Defendant's Notice of Security Incident, dated July 24, 2023, on or about that date. Plaintiff's notice stated that her name, gender, Social Security number, date of birth, address, and policy numbers were impacted.

56. As a result of the Data Breach, Plaintiff's sensitive information was accessed and/or acquired by an unauthorized actor and subsequently published on the dark web. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff will have to worry about when and how her sensitive information may be shared or used to her detriment.

57. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Security Incident and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

58. Additionally, Plaintiff is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

59. Plaintiff stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

60. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

61. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

62. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

63. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

64. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals in the United States and its territories whose PII was accessed and/or acquired in the data incident that is the subject of

> the Notice of Security Incident that Defendant sent to Plaintiff and Class Members on or around July 24, 2023 (the "Nationwide Class").

65. Plaintiff also proposes the following California Subclass definition, subject to amendment as appropriate:

> All California residents whose PII was accessed and/or acquired in the data incident that is the subject of the Notice of Security Incident that Defendant sent to Plaintiff and Class Members on or around July 24, 2023 (the "California Subclass").

66. The Nationwide Class and California Subclass are referred to collectively as the "Class" and members of the Nationwide Class and California Subclass are referred to collectively as "Class Members."

67. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

68. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

69. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. Defendant reported to the Delaware Attorney General that 1,386 Delaware residents were impacted in the Data Breach, and the Class is apparently identifiable within Defendant's records.

70. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. whether Defendant had duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. when Defendant actually learned of the Data Breach;

f. whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

71. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

72. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

73. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

74. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

75. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

76. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

77. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

78. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

79. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

80. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. whether Defendant breached the implied contract;

f. whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

81. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80. Defendant requires its customers, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of providing its life insurance services.

82. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

83. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

84. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to

unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

85. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Nationwide Class.

86. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special relationship arose because Defendant acquired Plaintiff's and the Nationwide Class's confidential PII in the course of its business practices.

87. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Nationwide Class.

88. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

89. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that PII, the necessity for encrypting PII shared with third parties, and the necessity for ensuring such third parties maintained the PII in encrypted form.

90. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of

Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendant.

91. Plaintiff and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

92. Defendant was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

93. Defendant had and continue to have a duty to adequately disclose that the PII of Plaintiff and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to: (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties; and (ii) prepare for the sharing and detrimental use of their sensitive information.

94. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Nationwide Class.

95. Defendant has admitted that the PII of Plaintiff and the Nationwide Class was wrongfully lost and disclosed to unauthorized third parties as a result of the Data Breach.

96. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Nationwide Class during the time the PII was within Defendant's possession or control.

97. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

98. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Nationwide Class in the face of increased risk of theft.

99. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

100. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

101. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Nationwide Class would not have been compromised.

102. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

103. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost

opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

104. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

105. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

106. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

107. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

108. Defendant's Privacy Policy states "[w]e maintain physical, electronic, and procedural safeguards to protect your [non-public personal information]."

109. In obtaining life insurance from Defendant, Plaintiff and the Nationwide Class provided and entrusted their PII to Defendant.

110. Defendant required Plaintiff and the Nationwide Class to provide and entrust their PII as a condition of obtaining life insurance from Defendant.

111. In so doing, Plaintiff and the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiff and the Nationwide Class if their PII had been compromised or stolen.

112. Plaintiff and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

113. Defendant breached the implied contracts it made with Plaintiff and the Nationwide Class by failing to implement appropriate technical and organizational security measures designed to protect their PII against accidental or unlawful unauthorized disclosure or unauthorized access and otherwise failing to safeguard and protect their PII.

114. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their confidential information; ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and

economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity-theft insurance; time spent scrutinizing bank statements, credit-card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

115. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Violations of the New York General Business Law §349
(On Behalf of Plaintiff and the Nationwide Class)

116. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

117. Defendant's Privacy Policy states "[w]e maintain physical, electronic, and procedural safeguards to protect your [non-public personal information]."

118. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law §349(a), including but not limited to misrepresenting that it would maintain physical, electronic, and procedural safeguards to protect the PII while not encrypting the PII and not ensuring that third parties with which it shared the PII would maintain it in encrypted form.

119. Defendant knew or should have known that its data-security practices were inadequate to safeguard the PII that Plaintiff and the Nationwide Class entrusted to Defendant, and that risk of a data breach or theft was highly likely.

120. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

121. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and the Nationwide Class) regarding the protection of their PII.

122. The representations upon which consumers (including Plaintiff and the Nationwide Class) relied were material representations (*e.g.*, as to Defendant's adequate protection of PII), and consumers (including Plaintiff and the Nationwide Class) relied on those representations to their detriment.

123. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and the Nationwide Class have been harmed, in that their PII was exposed to an unauthorized individual, which resulted in profound vulnerability to their personal information and other financial accounts.

124. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, the PII of Plaintiff and the Nationwide Class was disclosed to third parties without authorization, which has caused and will continue to cause damage to Plaintiff and the Nationwide Class.

125. Plaintiff and the Nationwide Class seek relief under N.Y. Gen. Bus. Law §349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

COUNT IV
VIOLATION OF CALIFORNIA'S CONSUMER PRIVACY ACT,
Cal. Civ. Code §1798.100 *et seq.*
(On Behalf of Plaintiff and the California Subclass)

126. Plaintiff and the California Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

127. Plaintiff brings this count on behalf of the California Subclass.

128. Through the above-detailed conduct, Defendant violated California's Consumer Privacy Act ("CCPA") by subjecting the nonencrypted and nonredacted Personal and Medical Information of Plaintiff and Class Members to unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature and protection of that information. Cal. Civ. Code §1798.150(a).

129. In accordance with Cal. Civ. Code §1798.150(b), prior to the filing of this Complaint, Plaintiff's counsel served Defendant with notice of these CCPA violations by certified mail, return receipt requested.

130. On behalf of the California Subclass members, Plaintiff seeks injunctive relief in the form of an order enjoining Defendant from continuing to violate the CCPA. If Defendant fails to respond to Plaintiff's notice letter or agree to rectify the violations detailed above, Plaintiff also will seek actual, punitive, and statutory damages, restitution, attorneys' fees and costs, and any other relief the Court deems proper as a result of Defendant's CCPA violations.

COUNT V
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Nationwide Class)

131. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 80.

132. Under the Declaratory Judgment Act, 28 U.S.C. §2201 *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

133. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and the Nationwide Class's PII and whether Defendant is currently maintaining data-security measures adequate to protect Plaintiff and the Nationwide Class from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data-security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and remains at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

134. Plaintiff and the Nationwide Class have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including: (i) Defendant's failure to encrypt Plaintiff's and the Nationwide Class's PII, including Social Security numbers; and (ii) Defendant's failure to ensured that third parties with which Defendant shared the PII stored it in encrypted form.

135. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII of Plaintiff and the Nationwide Class;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiff and the Nationwide Class harm.

136. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

a. audit, test, and train its data security personnel regarding any new or modified procedures; and

b. implement an education and training program for appropriate employees regarding cybersecurity.

137. If an injunction is not issued, Plaintiff and the Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at one of the third parties with which Defendant shares PII. The risk of another such breach is real, immediate, and substantial. If another such breach occurs, Plaintiff and the Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

138. The hardship to Plaintiff and the Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff and the Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

139. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff, the Class, and others whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and California Subclass, and appointing Plaintiff and her Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide

to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

vi. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

vii. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

DATED: December 14, 2023

Respectfully Submitted,

/s/Joseph P. Guglielmo
Joseph P. Guglielmo
SCOTT+SCOTT ATTORNEYS AT LAW
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: (212) 223-4478
jguglielmo@scott-scott.com

Karen Hanson Riebel (MN #0219770)*
Kate M. Baxter-Kauf (MN #0392037)*
Maureen Kane Berg (MN#033344X)*
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com
mkberg@locklaw.com

Jonathan M. Jagher*
FREED KANNER LONDON & MILLEN LLC
923 Fayette Street
Conshohocken, PA 19428
Telephone: (610) 234-6486
jjagher@fklmlaw.com

Andrea R. Gold*
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue NW,
Suite 1010
Washington, DC 20006
Phone: (202) 973-0900
Fax (202) 073-0950
agold@tzlegal.com

Attorneys for Plaintiff

**Pro Hac Vice* application forthcoming